

Document technique sur Wireshark

Par

Grégoire LE BARON

Table des matières :

1- Introduction

2- Modèle OSI

3- Installation

a) Prérequis

b) Installation

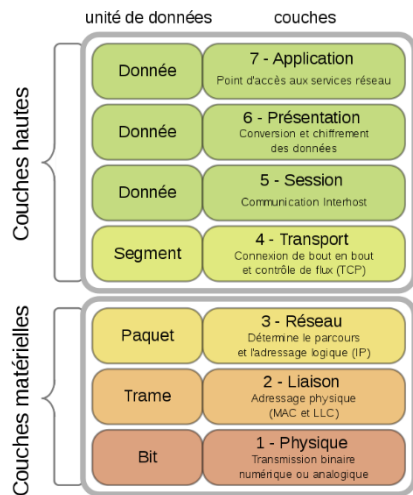
4- Fonctionnement

5- Fonctionnalités

1- Introduction

Wireshark est un logiciel open source permettant d'écouter les trames circulant sur un réseau ainsi que de les analyser. L'avantage de Wireshark est qu'il dispose une interface graphique.

2- Le modèle OSI



Le modèle OSI (Open Systems Interconnection) se divise en deux parties. Nous retrouvons en premier lieu les couches matérielles :

- 1- Physique : Transmission bit par bit entre l'émetteur et récepteur
- 2- Liaison : Contient l'adresse MAC propre à chaque périphérique
- 3- Réseau : Contient l'adresse IP propre à chaque connexion

Ensuite, nous retrouvons les couches hautes :

- 4- Transport : Contient le protocole TCP, qui permet de confirmer la réception des données.
- 5- Session : Cette couche gère les fichiers partagés sur le réseau
- 6- Présentation : Permet la mise en forme des données
- 7- Application : Correspond à l'interface entre la machine et l'utilisateur

Chaque niveau n'est pas indépendant des uns des autres. En effet, chaque protocole contient les protocoles inférieurs.

3- Installation

a) Prérequis

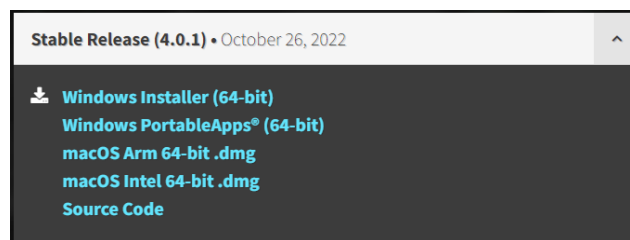
Afin d'installer le logiciel Wireshark, il est nécessaire d'avoir un système d'exploitation ainsi qu'une connexion internet.

D'un point de vue équipement, il est nécessaire d'avoir :

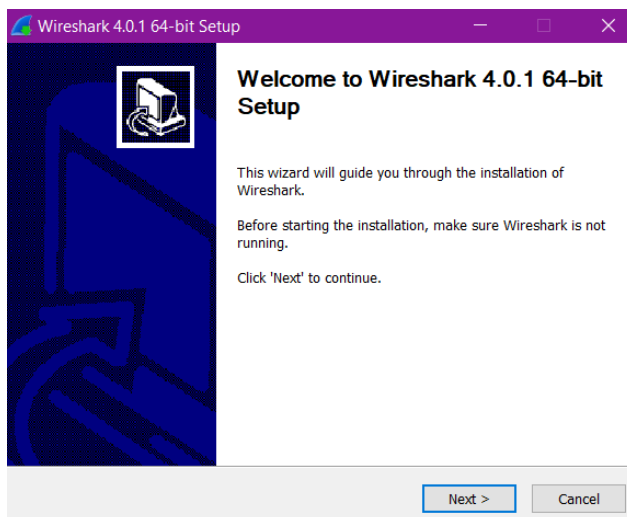
- Processeur 64bit AMD64/x86-64 ou 32bit x86.
- 62,5 Mo d'espace disponible sur le disque dur
- 62,5 Mo de RAM disponible

b) Installation

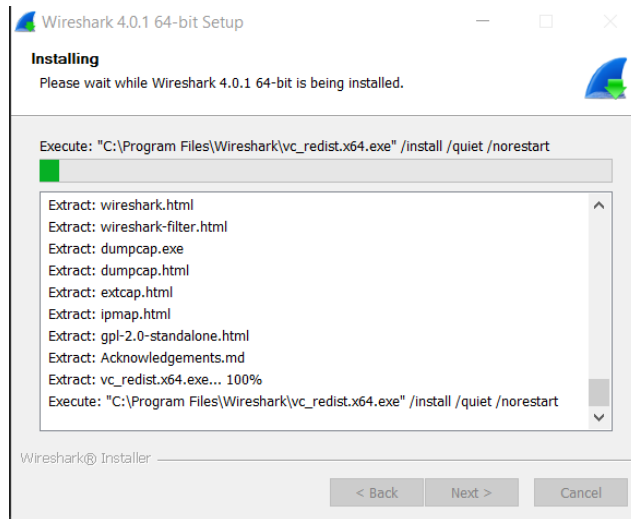
Pour installer ce logiciel, nous nous dirigeons sur le site : <https://wireshark.org>.



Nous sélectionnons le fichier qui est compatible avec le système d'exploitation de notre machine. Dans mon cas il s'agit du fichier « Windows Installer (64-bits) ».



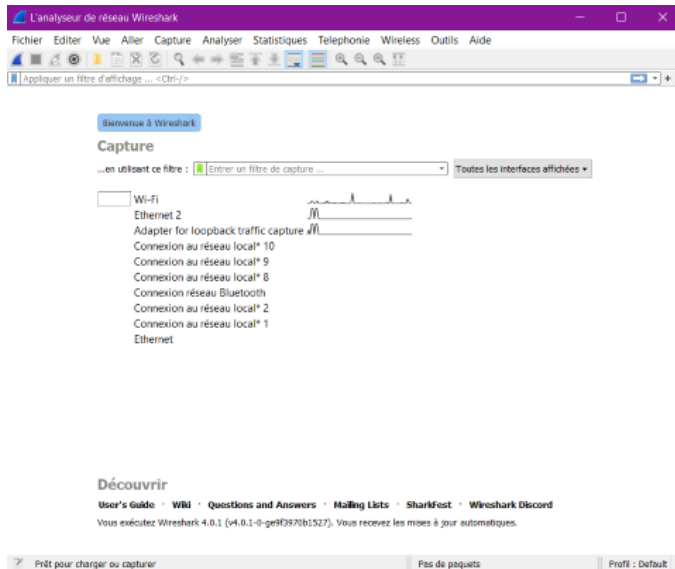
Ensuite, nous lançons le fichier précédemment installé et nous suivons les étapes. On sélectionne le bouton « Next > » à chaque étape car tout est déjà pré-coché.



Nous arrivons à l'étape finale ou le logiciel décompresse tous les fichiers.

4- Fonctionnement

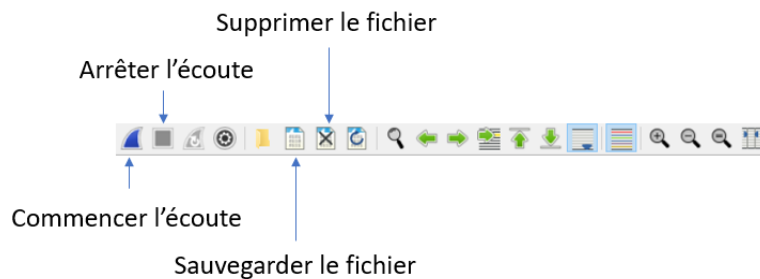
Nous exécutons le logiciel en tant qu'administrateur. Nous obtenons cette première page.



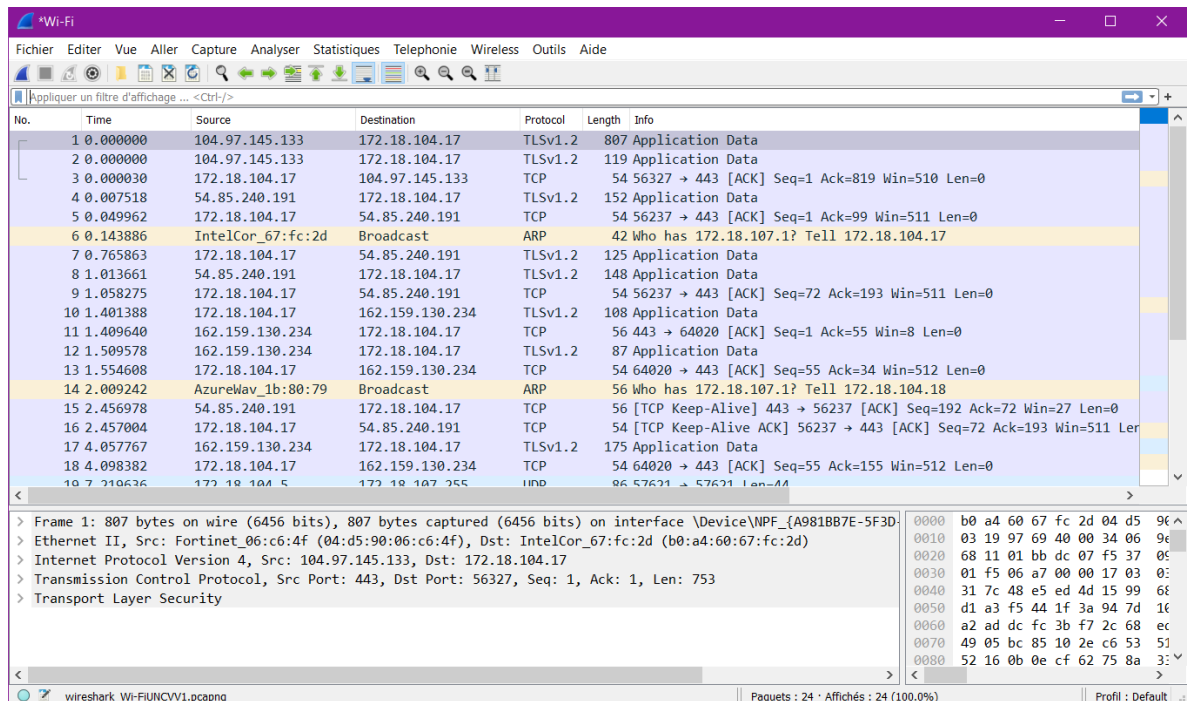
Nous observons sur cette capture d'écran que le logiciel écoute plusieurs adaptateurs réseaux.

Pour la suite de cette documentation technique, nous allons analyser le Wi-Fi.

Nous retrouvons en premier lieu différentes icônes permettant de gérer l'écoute.



Document technique Wireshark



Ensuite, chaque ligne correspond à une trame. Nous observons que chaque colonne permet de communiquer une information sur la trame. Nous avons dans l'ordre :

- Le numéro de trame
- Le temps, sachant que t=0 correspond au lancement de l'écoute
- La source de la trame
- La destination de la trame
- Le protocole maximal utilisé
- La longueur de la trame
- Des informations complémentaires

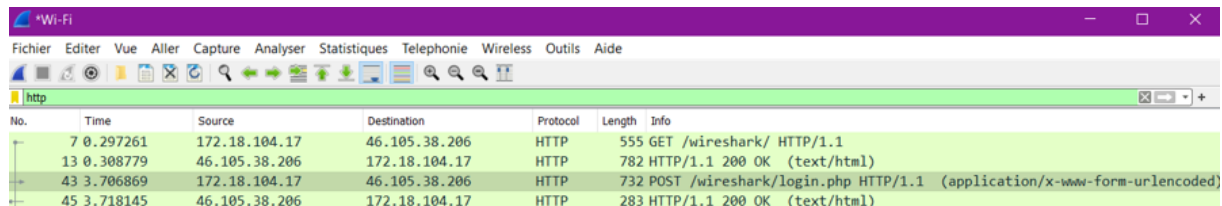
Enfin, en bas de la page, nous retrouvons les détails de la trame sélectionnée. Nous retrouvons chaque protocole inférieur au protocole maximal de la trame. A droite, nous retrouvons les données en hexadécimale.

5- Fonctionnalités

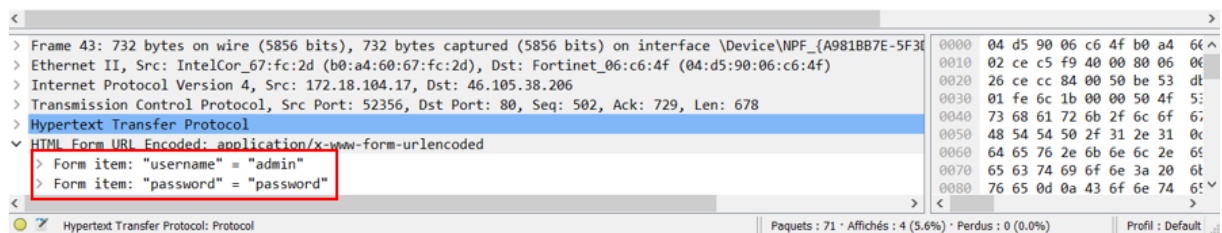
Wireshark dispose de plusieurs filtres qui permet d'optimiser l'analyse de nos données. Nous pouvons concaténer plusieurs filtres à l'aide des caractères « && » ou « and ».

Nous pouvons également exclure certains paramètres à l'aide des caractères « not » ou « ! ».

Chaque trame est surlignée en fonction du protocole.



No.	Time	Source	Destination	Protocol	Length	Info
7	0.297261	172.18.104.17	46.105.38.206	HTTP	555	GET /wireshark/ HTTP/1.1
13	0.308779	46.105.38.206	172.18.104.17	HTTP	782	HTTP/1.1 200 OK (text/html)
43	3.706869	172.18.104.17	46.105.38.206	HTTP	732	POST /wireshark/login.php HTTP/1.1 (application/x-www-form-urlencoded)
45	3.718145	46.105.38.206	172.18.104.17	HTTP	283	HTTP/1.1 200 OK (text/html)



> Frame 43: 732 bytes on wire (5856 bits), 732 bytes captured (5856 bits) on interface \Device\NPF_{A981BB7E-5F3C-4000-8000-000000000000} (04:d5:90:06:c6:4f) (04:d5:90:06:c6:4f)

> Ethernet II, Src: IntelCor_67:fc:2d (b0:a4:60:67:fc:2d), Dst: Fortinet_06:c6:4f (04:d5:90:06:c6:4f)

> Internet Protocol Version 4, Src: 172.18.104.17, Dst: 46.105.38.206

> Transmission Control Protocol, Src Port: 52356, Dst Port: 80, Seq: 502, Ack: 729, Len: 678

> Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

> Form item: "username" = "admin"

> Form item: "password" = "password"

Cet outil est en mesure de récupérer les logins et passwords d'un site http comme nous pouvons le voir sur la capture d'écran précédente.